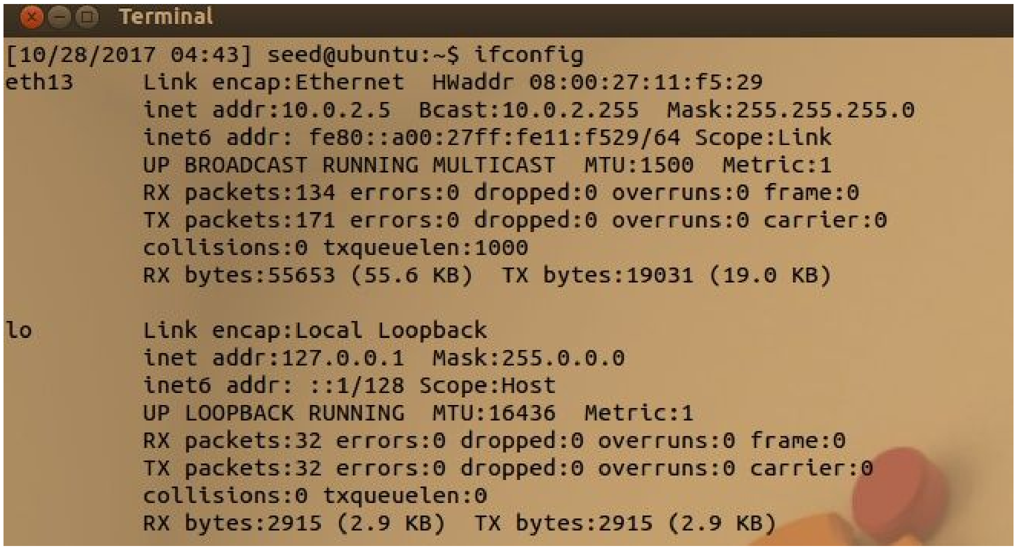
Adrian Cuellar

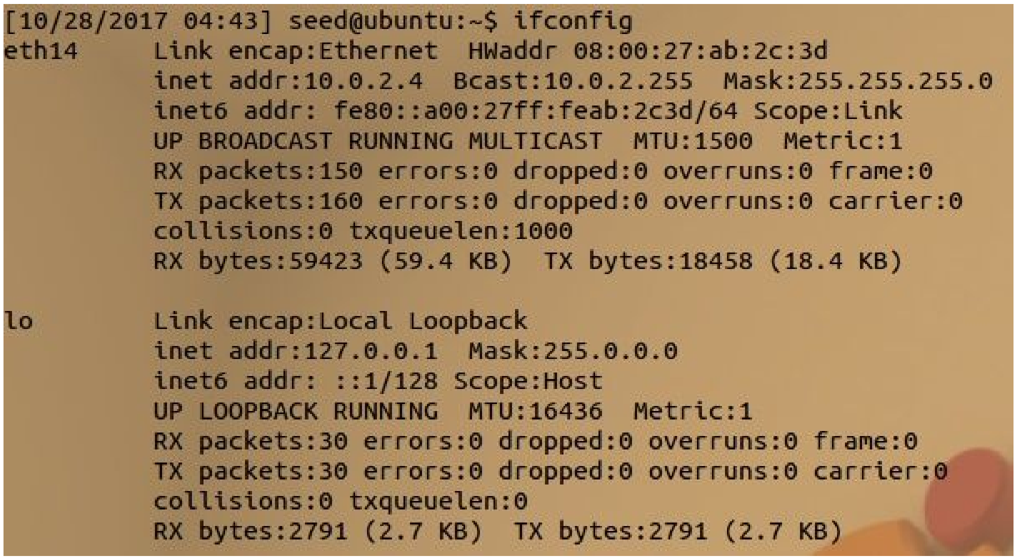
Problem 1.

Original



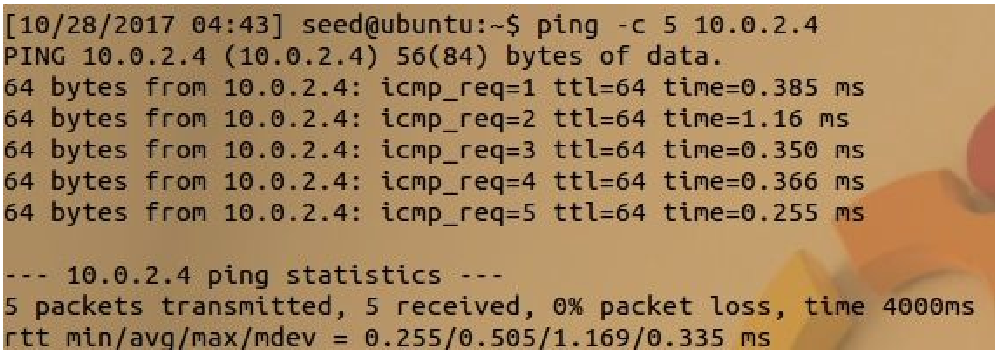
```
[10/28/2017 04:43] seed@ubuntu:~$ ifconfig
eth13     Link encap:Ethernet  HWaddr 08:00:27:11:f5:29
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe11:f529/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:134 errors:0 dropped:0 overruns:0 frame:0
          TX packets:171 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:55653 (55.6 KB)  TX bytes:19031 (19.0 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:32 errors:0 dropped:0 overruns:0 frame:0
          TX packets:32 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2915 (2.9 KB)  TX bytes:2915 (2.9 KB)
```

Copy



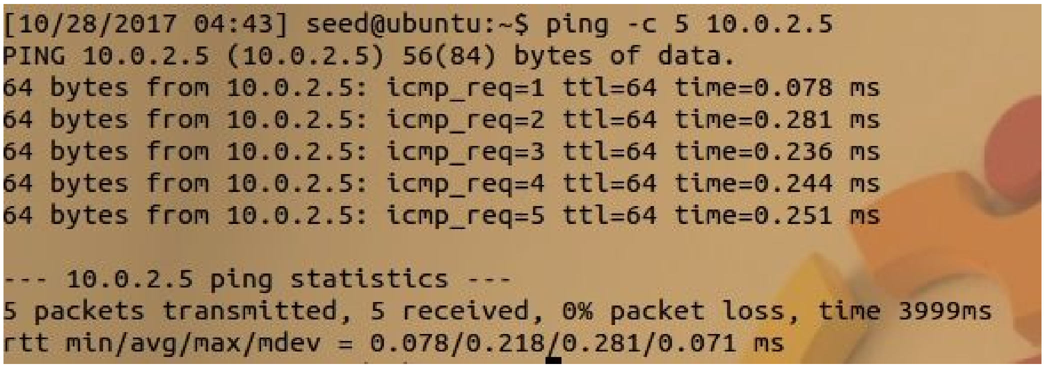
```
[10/28/2017 04:43] seed@ubuntu:~$ ifconfig
eth14     Link encap:Ethernet  HWaddr 08:00:27:ab:2c:3d
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feab:2c3d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:150 errors:0 dropped:0 overruns:0 frame:0
          TX packets:160 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:59423 (59.4 KB)  TX bytes:18458 (18.4 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:30 errors:0 dropped:0 overruns:0 frame:0
          TX packets:30 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2791 (2.7 KB)  TX bytes:2791 (2.7 KB)
```

Original



```
[10/28/2017 04:43] seed@ubuntu:~$ ping -c 5 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_req=1 ttl=64 time=0.385 ms
64 bytes from 10.0.2.4: icmp_req=2 ttl=64 time=1.16 ms
64 bytes from 10.0.2.4: icmp_req=3 ttl=64 time=0.350 ms
64 bytes from 10.0.2.4: icmp_req=4 ttl=64 time=0.366 ms
64 bytes from 10.0.2.4: icmp_req=5 ttl=64 time=0.255 ms

--- 10.0.2.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.255/0.505/1.169/0.335 ms
```

Copy

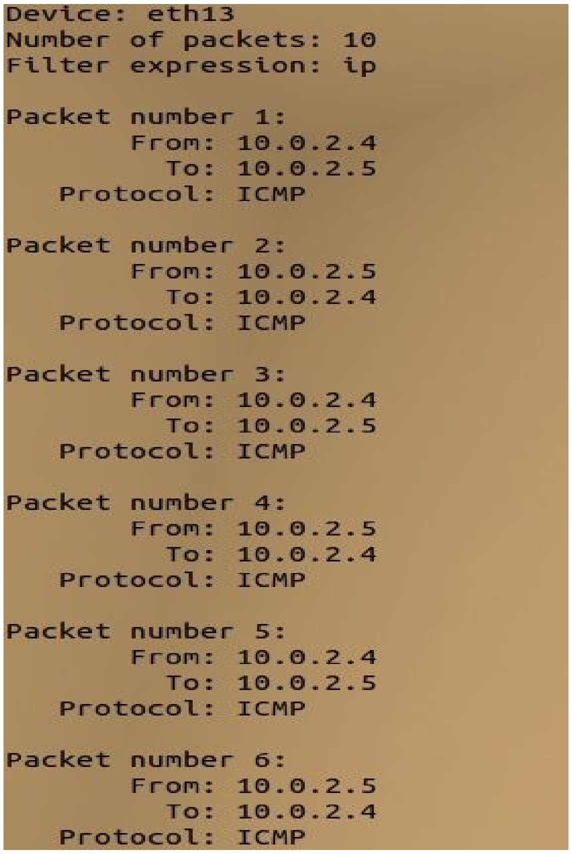


```
[10/28/2017 04:43] seed@ubuntu:~$ ping -c 5 10.0.2.5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data.
64 bytes from 10.0.2.5: icmp_req=1 ttl=64 time=0.078 ms
64 bytes from 10.0.2.5: icmp_req=2 ttl=64 time=0.281 ms
64 bytes from 10.0.2.5: icmp_req=3 ttl=64 time=0.236 ms
64 bytes from 10.0.2.5: icmp_req=4 ttl=64 time=0.244 ms
64 bytes from 10.0.2.5: icmp_req=5 ttl=64 time=0.251 ms

--- 10.0.2.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.078/0.218/0.281/0.071 ms
```

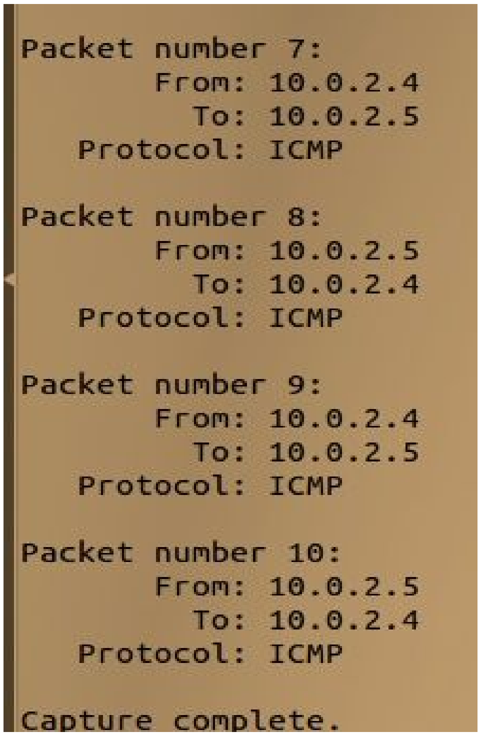
Problem 2.

The pcap library is used to essentially look up an interface to ‘sniff’ on and to dissect or save or print any of the packets that are sent to the interface that is being ‘sniffed’ on. It can sniff either all of the incoming packets or packets of a specific type, or packings coming into a specific port, etc.

When I run the packet sniffer without admin permission the program fails to start as eth13 cannot be opened as I do not have permission to capture on that device.

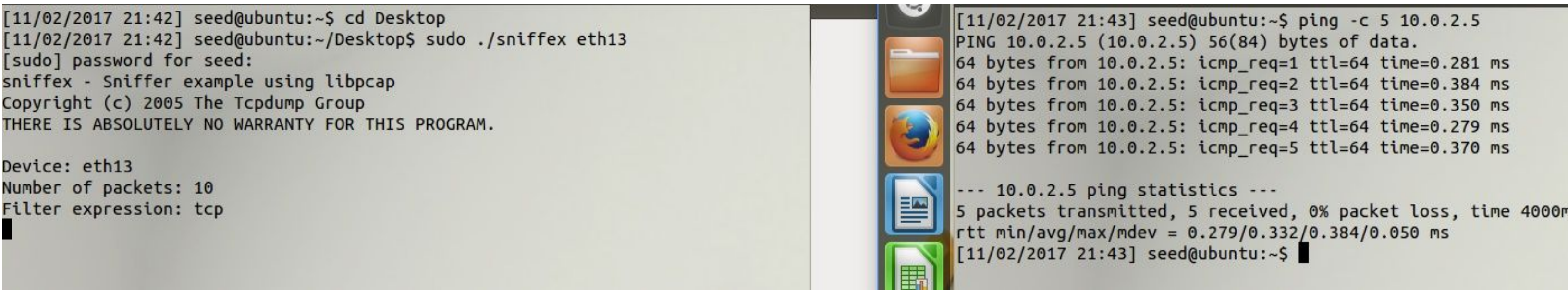


```
Device: eth13
Number of packets: 10
Filter expression: ip

Packet number 1:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: ICMP

Packet number 2:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: ICMP

Packet number 3:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: ICMP

Packet number 4:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: ICMP

Packet number 5:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: ICMP

Packet number 6:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: ICMP
```



```
Packet number 7:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: ICMP

Packet number 8:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: ICMP

Packet number 9:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: ICMP

Packet number 10:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: ICMP

Capture complete.
```

When only TCP packets are captured:

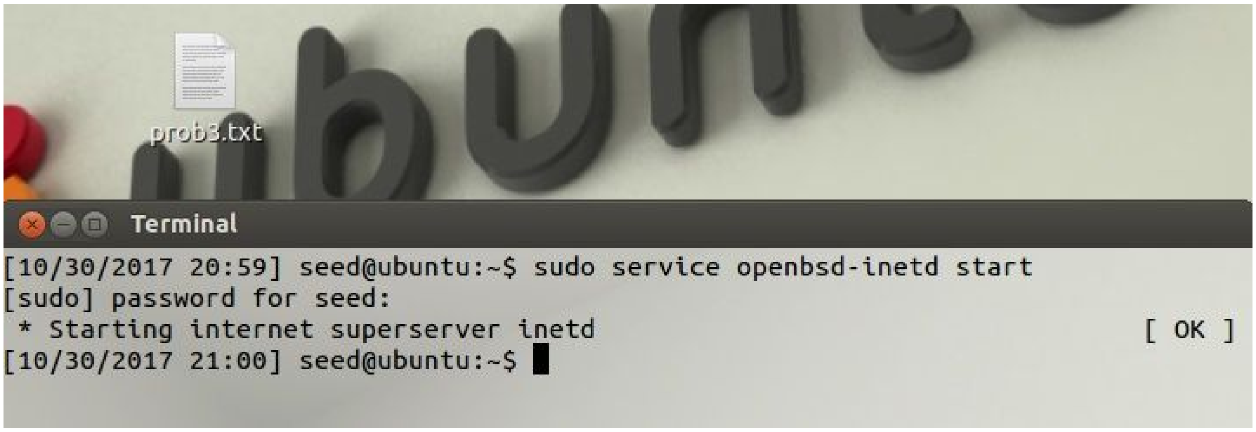


```
[11/02/2017 21:42] seed@ubuntu:~$ cd Desktop
[11/02/2017 21:42] seed@ubuntu:~/Desktop$ sudo ./sniffex eth13
[sudo] password for seed:
sniffex - Sniffer example using libpcap
Copyright (c) 2005 The Tcpdump Group
THERE IS ABSOLUTELY NO WARRANTY FOR THIS PROGRAM.

Device: eth13
Number of packets: 10
Filter expression: tcp
```

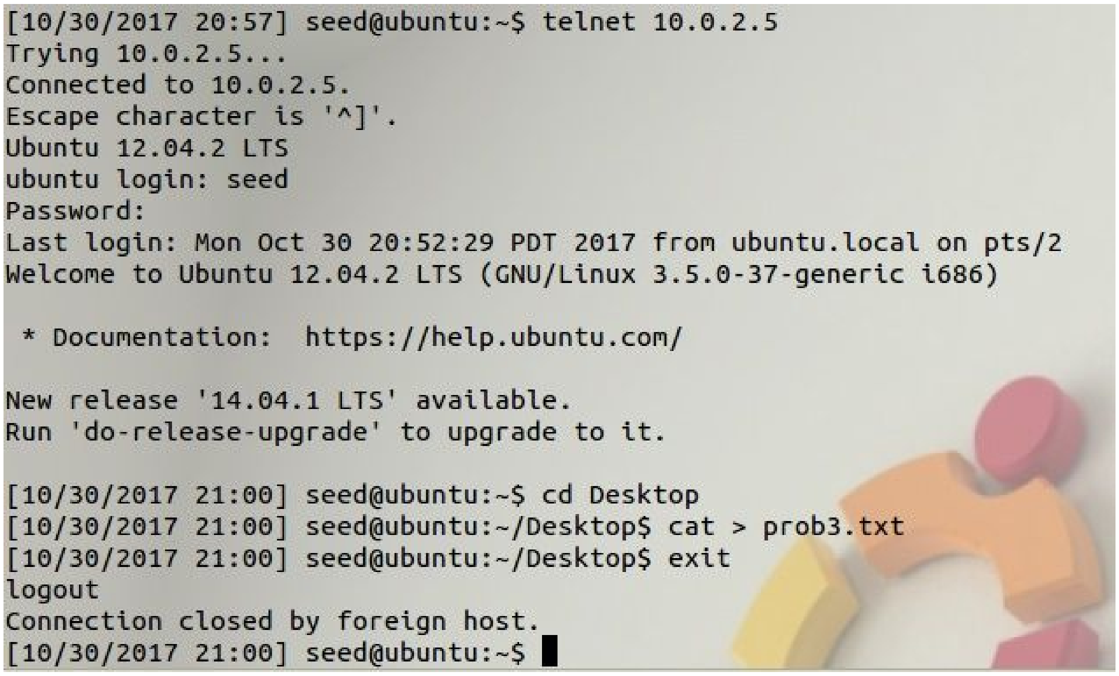
```
[11/02/2017 21:43] seed@ubuntu:~$ ping -c 5 10.0.2.5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data.
64 bytes from 10.0.2.5: icmp_req=1 ttl=64 time=0.281 ms
64 bytes from 10.0.2.5: icmp_req=2 ttl=64 time=0.384 ms
64 bytes from 10.0.2.5: icmp_req=3 ttl=64 time=0.350 ms
64 bytes from 10.0.2.5: icmp_req=4 ttl=64 time=0.279 ms
64 bytes from 10.0.2.5: icmp_req=5 ttl=64 time=0.370 ms

--- 10.0.2.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000m
rtt min/avg/max/mdev = 0.279/0.332/0.384/0.050 ms
[11/02/2017 21:43] seed@ubuntu:~$
```

Nothing is sniffed when being pinged.

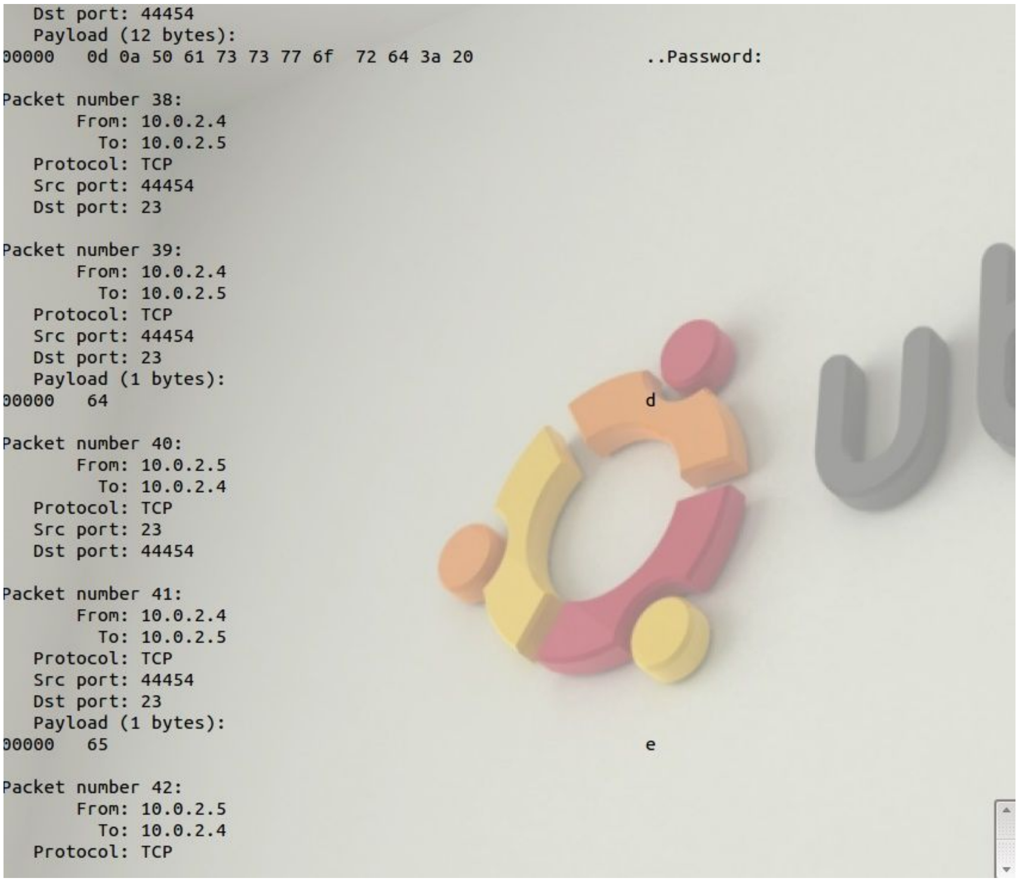
Problem 3.



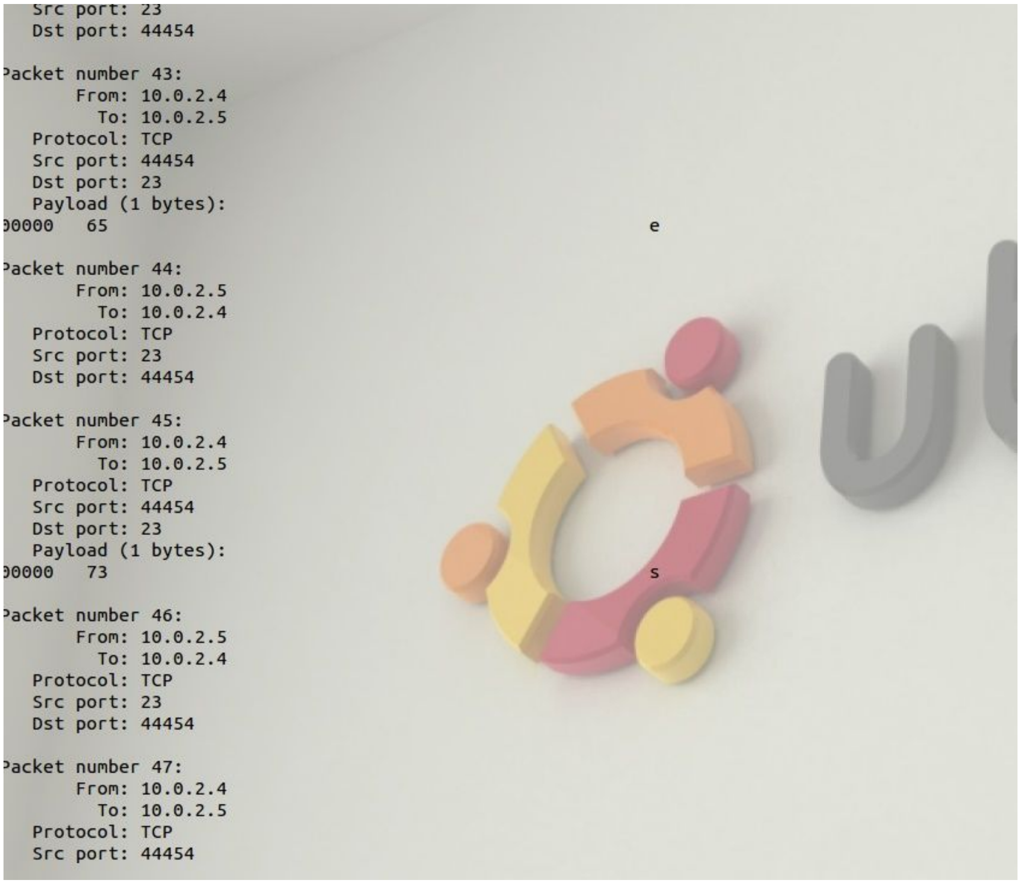
```
[10/30/2017 20:59] seed@ubuntu:~$ sudo service openbsd-inetd start
[sudo] password for seed:
 * Starting internet superserver inetd                                   [ OK ]
[10/30/2017 21:00] seed@ubuntu:~$
```



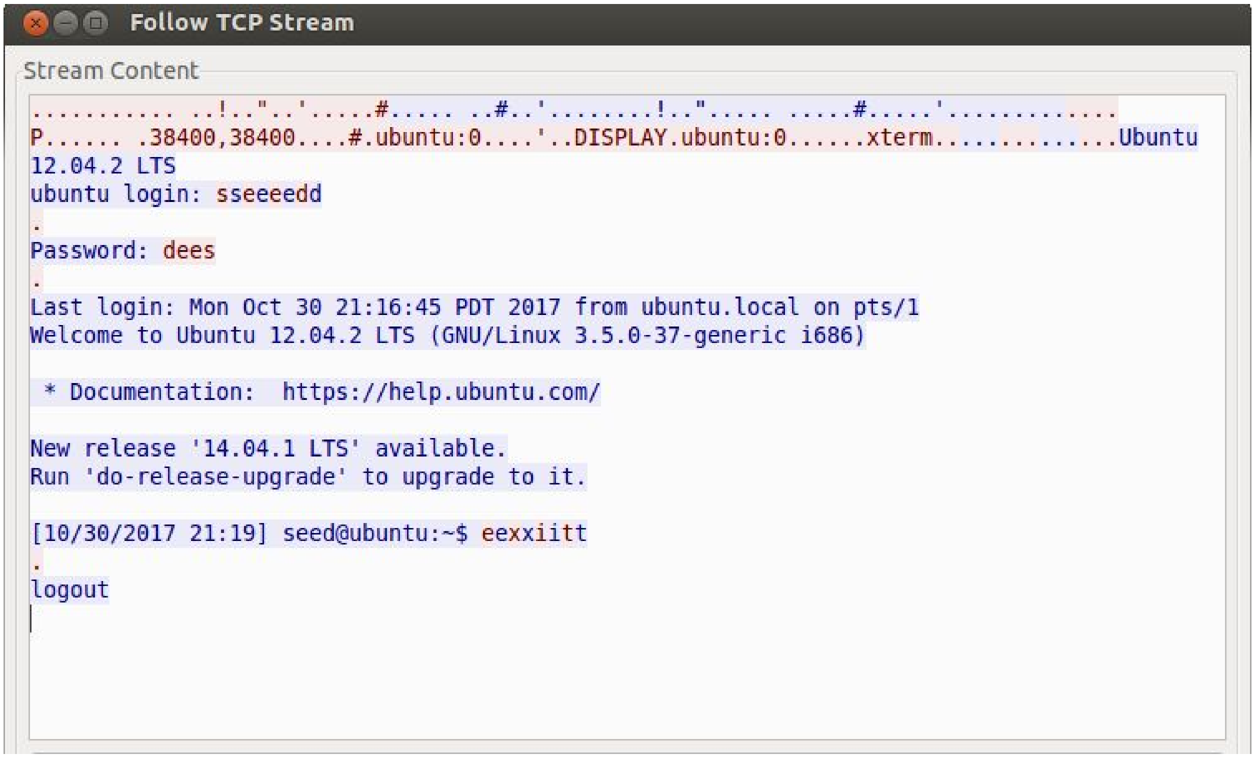
```
[10/30/2017 20:57] seed@ubuntu:~$ telnet 10.0.2.5
Trying 10.0.2.5...
Connected to 10.0.2.5.
Escape character is '^]'.
Ubuntu 12.04.2 LTS
ubuntu login: seed
Password:
Last login: Mon Oct 30 20:52:29 PDT 2017 from ubuntu.local on pts/2
Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.5.0-37-generic i686)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

[10/30/2017 21:00] seed@ubuntu:~$ cd Desktop
[10/30/2017 21:00] seed@ubuntu:~/Desktop$ cat > prob3.txt
[10/30/2017 21:00] seed@ubuntu:~/Desktop$ exit
logout
Connection closed by foreign host.
[10/30/2017 21:00] seed@ubuntu:~$
```



```
   Dst port: 44454
   Payload (12 bytes):
00000   0d 0a 50 61 73 73 77 6f  72 64 3a 20                ..Password:

Packet number 38:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 44454
   Dst port: 23

Packet number 39:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 44454
   Dst port: 23
   Payload (1 bytes):
00000   64                                                  d

Packet number 40:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 23
   Dst port: 44454

Packet number 41:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 44454
   Dst port: 23
   Payload (1 bytes):
00000   65                                                  e

Packet number 42:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
```



```
   Src port: 23
   Dst port: 44454

Packet number 43:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 44454
   Dst port: 23
   Payload (1 bytes):
00000   65                                                  e

Packet number 44:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 23
   Dst port: 44454

Packet number 45:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 44454
   Dst port: 23
   Payload (1 bytes):
00000   73                                                  s

Packet number 46:
       From: 10.0.2.5
         To: 10.0.2.4
   Protocol: TCP
   Src port: 23
   Dst port: 44454

Packet number 47:
       From: 10.0.2.4
         To: 10.0.2.5
   Protocol: TCP
   Src port: 44454
```

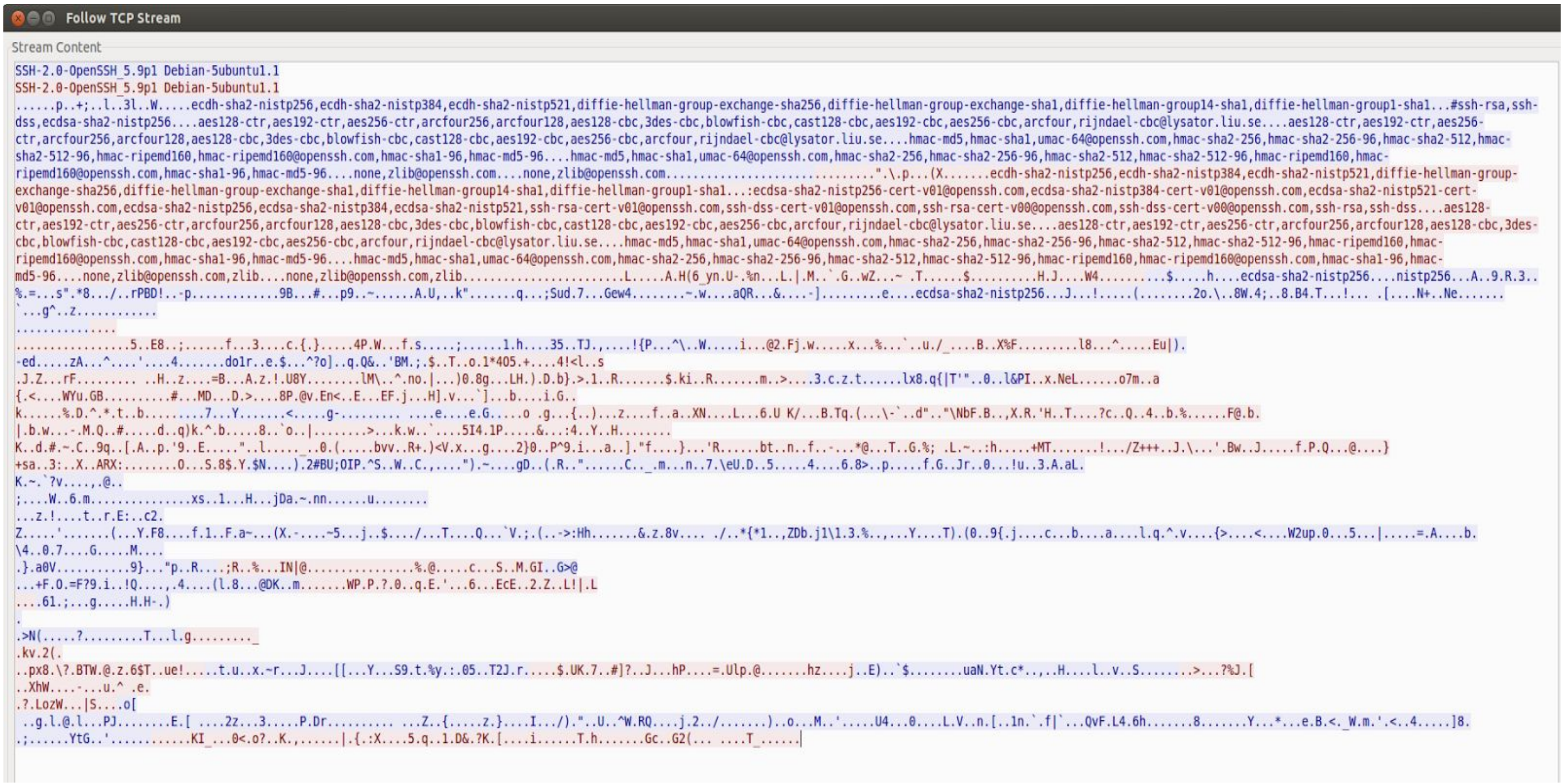


```
..........  ..!..".'.....#.....  ..#..'........!..".....  .....#.....'.............
P......  .38400,38400....#.ubuntu:0....'..DISPLAY.ubuntu:0......xterm..............Ubuntu
12.04.2 LTS
ubuntu login: sseeeedd
.
Password: dees
.
Last login: Mon Oct 30 21:16:45 PDT 2017 from ubuntu.local on pts/1
Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.5.0-37-generic i686)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

[10/30/2017 21:19] seed@ubuntu:~$ eexxiitt
.
logout
```

Considering the results that both times I could find the user’s password logging in, I definitely would not recommend using telnet as a method of remotely accessing a system, it is too vulnerable with how it freely transmits the information with no encryption or anything along the way to others could find the user’s password as well. It is just too unsafe.

Problem 4.

Cannot find the user’s password while using SSH.



```
SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.1
SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.1
......p..+;..l..3l..W.....ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1...#ssh-rsa,ssh-
dss,ecdsa-sha2-nistp256....aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se....aes128-ctr,aes192-ctr,aes256-
ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se....hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-sha2-256,hmac-sha2-256-96,hmac-sha2-512,hmac-
sha2-512-96,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96....hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-sha2-256,hmac-sha2-256-96,hmac-sha2-512,hmac-sha2-512-96,hmac-ripemd160,hmac-
ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96....none,zlib@openssh.com....none,zlib@openssh.com.............................".\.p...(X.......ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-
exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1...:ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-
v01@openssh.com,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-rsa-cert-v01@openssh.com,ssh-dss-cert-v01@openssh.com,ssh-rsa-cert-v00@openssh.com,ssh-dss-cert-v00@openssh.com,ssh-rsa,ssh-dss....aes128-
ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se....aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-
cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se....hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-sha2-256,hmac-sha2-256-96,hmac-sha2-512,hmac-sha2-512-96,hmac-ripemd160,hmac-
ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96....hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-sha2-256,hmac-sha2-256-96,hmac-sha2-512,hmac-sha2-512-96,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-
md5-96....none,zlib@openssh.com,zlib....none,zlib@openssh.com,zlib........................L.....A.H(6_yn.U-.%n...L.|.M..`.G..wZ...~ .T......$.........H.J....W4..........$.....h....ecdsa-sha2-nistp256....nistp256...A..9.R.3..
%.=...s".*8.../..rPBD!..-p............9B...#...p9..~......A.U,..k"......q...;Sud.7...Gew4........~.w....aQR...&....-]........e....ecdsa-sha2-nistp256...J...!.....(.......2o.\..8W.4;..8.B4.T...!... .[....N+..Ne.......
`...g^..z............
...............
.................5..E8..;......f...3....c.{.}.....4P.W...f.s.....;......1.h....35..TJ.,....!{P...^\..W.....i...@2.Fj.w.....x...%...`..u./_....B..X%F.........l8...^.....Eu|).
-ed.....zA...^....'....4.......do1r..e.$...^?o]..q.Q&..'BM.;.$..T..o.1*405.+....4!<l..s
.J.Z...rF......... ..H..z....=B...A.z.!.U8Y........lM\..^.no.|...)0.8g...LH.).D.b}.>.1..R.......$.ki..R.......m..>....3.c.z.t......lx8.q{|T'"..0..l&PI..x.NeL......o7m..a
{.<....WYu.GB..........#...MD...D.>....8P.@v.En<..E...EF.j...H].v...`]...b....i.G..
k......%.D.^.*.t..b.........7...Y.......<.....g-......... ....e....e.G.....o .g...{..)...z....f..a..XN....L...6.U K/...B.Tq.(...\-`..d".."\NbF.B..,X.R.'H..T....?c..Q..4..b.%......F@.b.
|.b.w...-.M.Q..#.....d..q)k.^.b.....8..`o..|........>...k.w..`....5I4.1P.....&...:4..Y..H........
K..d.#.~.C..9q..[.A..p.'9..E....."..l....._..0.(.....bvv..R+.)<V.x...g....2}0..P^9.i...a..]."f....}...'R......bt..n..f..-...*@...T..G.%; .L.~..:h.....+MT.......!.../Z++..J.\...'.Bw..J.....f.P.Q...@....}
+sa..3:..X..ARX:........O...S.8$.Y.$N....).2#BU;OIP.^S..W..C.,....").~....gD..(.R.."......C.._.m...n..7.\eU.D..5.....4....6.8>..p.....f.G..Jr..0...!u..3.A.aL.
K.~.`?v....,.@..
;....W..6.m...............xs..1...H...jDa.~.nn......u........
...z.!....t..r.E:..c2.
Z.....'.......(...Y.F8....f.1..F.a~...(X.-....~5...j..$..../...T....Q...`V.;.(..->:Hh.......&.z.8v.... ./..*{*1..,ZDb.j1\1.3.%..,...Y....T).(0..9{.j....c...b....a....l.q.^.v....{>....<....W2up.0...5...|.....=.A....b.
\4..0.7....G.....M....
.}.a0V...........9}..."p..R....;R..%...IN|@................%.@.....c...S..M.GI..G>@
...+F.O.=F?9.i..!Q....,.4....(l.8...@DK..m.......WP.P.?.0..q.E.'...6...EcE..2.Z..L!|.L
....61.;...g.....H.H-.)
.
.>N(.....?.........T...l.g........._
.kv.2(.
..px8.\?.BTW.@.z.6$T..ue!.....t.u..x.~r...J....[[...Y...S9.t.%y.:.05..T2J.r.....$.UK.7..#]?..J...hP....=.Ulp.@......hz....j..E)..`$........uaN.Yt.c*..,..H....l..v..S........>...?%J.[
..XhW....-...u.^ .e.
.?.LozW...|S....o[
 ..g.l.@.l...PJ........E.[ ....2z...3.....P.Dr.......... ...Z..{.....z.}....I.../)."..U..^W.RQ....j.2../.......)..o...M..'.....U4...0....L.V..n.[..1n.`.f|`...QvF.L4.6h.......8.......Y...*...e.B.<._W.m.'.<..4.....]8.
.;......YtG..'............KI_...0<.o?..K.,......|.{.:X....5.q..1.D&.?K.[....i......T.h.......Gc..G2(... ....T_......
```